THE LIE MODULE OF THE SYMMETRIC GROUP

KARIN ERDMANN AND KAI MENG TAN

ABSTRACT. We provide an upper bound of the dimension of the maximal projective submodule of the Lie module of the symmetric group of n letters in prime characteristic p, where $n = pk$ with $p \nmid k$.

1. INTRODUCTION

The Lie module of the symmetric group $\mathfrak{S}_n$ appears in many contexts; in particular it is closely related to the free Lie algebra. One possible approach is to view it as the right ideal of the group algebra $F\mathfrak{S}_n$, generated by the 'Dynkin-Specht-Wever element'

$$\omega_n := (1 - c_2)(1 - c_3) \cdots (1 - c_n)$$

where c_k is the k-cycle $(1, 2, \dots, k)$. We write $\mathrm{Lie}(n) = \omega_n F\mathfrak{S}_n$ for this Lie module.

It is well-known that $\omega_n^2 = n\omega_n$, so if n is non-zero in F then $\mathrm{Lie}(n)$ is a direct summand of the group algebra and hence is projective. We are interested in this module when F has prime characteristic p and when p divides n. In this case ω_n is nilpotent, and therefore $\mathrm{Lie}(n)$ always has non-projective summands, and its module structure is not well-understood in general.

The module $\mathrm{Lie}(n)$ is not only part of the algebraic literature, for example it has already appeared in the work of Witt [Wi] and Weber [We], it also occurs in the context of algebraic topology, as a homology group in spaces related to braid groups [C], configuration spaces and in the study of Goodwillie calculus [AM]; and in [AK], Arone and Kankaanrinta calculate the homology of $\mathfrak{S}_n$ with coefficients in $\mathrm{Lie}(n)$. They show that it is zero unless $n = p^k$, and that $H_*(\mathfrak{S}_{p^k}, \mathrm{Lie}(p^k))$ has a basis corresponding to admissible sequences of Steenrod operations of length k.

The main motivation for our paper comes from the work of Selick and Wu [SW1]. Their problem is to find natural homotopy decompositions of the loop suspension of a p-torsion suspension where p is a prime. In [SW1] it is proved that this problem is equivalent to the algebraic problem of finding natural coalgebra decompositions of the primitively generated tensor

Date: Nov 2009.
2000 *Mathematics Subject Classification.* 20C30.
The second author thanks the Mathematical Institute, Oxford, for its hospitality during his visit in 2006, during which most of the work appearing here was done, and acknowledges support by MOE's Academic Research Fund R-146-000-089-112.

algebras over the field with p elements. They determine the finest coalgebra decomposition of a tensor algebra (over arbitrary fields), which can be described as a functorial Poincarè-Birkhoff-Witt theorem [SW1, Theorem 6.5]. In order to compute the factors in this decomposition, one must know a maximal projective submodule, called $\mathrm{Lie}^{\max}(n)$, of the Lie module $\mathrm{Lie}(n)$.

Since $\mathrm{Lie}(n)$ is a finite-dimensional module, and since projective modules for symmetric groups are injective, there is a direct sum decomposition of the form $\mathrm{Lie}(n) = \mathrm{Lie}(n)_{pr} \oplus \mathrm{Lie}(n)_{pf}$, unique up to isomorphism, where $\mathrm{Lie}(n)_{pr}$ is projective and $\mathrm{Lie}(n)_{pf}$ does not have any non-zero projective summand. Then $\mathrm{Lie}^{\max}(n)$ is isomorphic to $\mathrm{Lie}(n)_{pr}$. As mentioned above, if p does not divide n then $\mathrm{Lie}(n) = \mathrm{Lie}(n)_{pr}$; on the other hand whenever p divides n, the summand $\mathrm{Lie}(n)_{pf}$ is non-zero (though, the homology of the symmetric group with coefficients in $\mathrm{Lie}(n)$, that is, with coefficients in $\mathrm{Lie}(n)_{pf}$, is zero if n is not a power of p).

The projective modules for the symmetric groups over fields of positive characteristic are not known. Their structure depends on the decomposition matrices for symmetric groups, and the determination of the latter is a famous open problem. According to [SW2], it would be interesting to know, even if the modules cannot be computed precisely, how quickly the dimensions grow, and whether or not the growth rate is exponential. Evidence in [SW2], for small cases in characteristic 2, is that $\mathrm{Lie}^{\max}(n)$ is relatively large compared with $\mathrm{Lie}(n)$ and this would correspond to factors in the functorial PBW theorem being relatively small.

When $n = pk$ and p does not divide k, a parametrisation of the indecomposable summands of $\mathrm{Lie}(n)_{pf}$ was given in [ES]. Here we exploit this result to obtain an upper bound for the dimension of $\mathrm{Lie}^{\max}(n)$. The general principle is quite easy. If P is a subgroup of a finite group G, then one may consider the restriction of any FG-module W to FP, which we denote as $\mathrm{Res}^G_P W$. Then $\mathrm{Res}^G_P(W_{pr})$ is a direct summand of $(\mathrm{Res}^G_P W)_{pr}$ and therefore

$$\dim W_{pr} \le \dim\,(\mathrm{Res}^G_P W)_{pr} \le \dim W - \dim\,(\mathrm{Res}^G_P W)_{pf}.$$

Thus, when $G = \mathfrak{S}_n$ and $W = \mathrm{Lie}(n)$, we have

$$\dim \mathrm{Lie}^{\max}(n) \le (n-1)! - \dim\,(\mathrm{Res}^{\mathfrak{S}_n}_P \mathrm{Lie}(n))_{pf}.$$

In this paper, we take P to be a Sylow p-subgroup of $\mathfrak{S}_n$, and we provide in particular a recursive formula for computing $\dim\,(\mathrm{Res}^{\mathfrak{S}_n}_P \mathrm{Lie}(n))_{pf}$.

We give an outline of this paper. After introducing notation, we reduce in Section 3 the problem of computing $\dim(\mathrm{Res}^{\mathfrak{S}_{kp}}_P \mathrm{Lie}(pk))_{pf}$ to that of computing the number of certain right cosets. Section 4 studies the Sylow p-subgroup P of $\mathfrak{S}_{pk}$, especially its elements of order p which are fixed-point-free as elements of $\mathfrak{S}_{pk}$. In Section 5, we obtain a 'good' subset containing a transversal of the right cosets which we wish to parametrise, and proceed to obtain a transversal in Section 6. We end the paper with a recursive formula for the dimension of $(\mathrm{Res}^{\mathfrak{S}_{kp}}_P \mathrm{Lie}(pk))_{pf}$, and we show that while this dimension grows exponentially with k, its ratio to $\dim(\mathrm{Lie}(kp))$ approaches zero as k tends to infinity. At present, no parametrisation of the indecomposable

summands of $\mathrm{Lie}(n)$ is known when n is divisible by p^2, therefore the problem of finding bounds for the dimension of $\mathrm{Lie}^{\max}(n)$ cannot be approached in the same way.

We refer the reader to [B] for the necessary background on representation theory of finite groups.

2. Notations

In this section, we introduce the notations to be used throughout this paper.

For $a, b \in \mathbb{Z}_{\geq 0}$ with $a < b$, let

$$\begin{aligned}
[a,b] &= \{x \in \mathbb{Z} \mid a \leq x \leq b\},\\
(a,b] &= \{x \in \mathbb{Z} \mid a < x \leq b\},\\
[a,b) &= \{x \in \mathbb{Z} \mid a \leq x < b\}.
\end{aligned}$$

We denote by $\mathfrak{S}_n$ the group of permutations of the set $[1,n]$. For $m < n$, we identify $\mathfrak{S}_m$ with the subgroup of $\mathfrak{S}_n$ fixing $(m,n]$ pointwise.

Let $a, b \in \mathbb{Z}^+$. For $\sigma \in \mathfrak{S}_a$, define $\sigma^{[b]} \in \mathfrak{S}_{ab}$ by

$$((i-1)b + j)\sigma^{[b]} = (i\sigma - 1)b + j$$

for all $i \in [1,a]$ and $j \in [1,b]$, so that $\sigma^{[b]}$ permutes the a successive blocks of size b in $[1,ab]$ according to σ. Clearly, the map $\sigma \mapsto \sigma^{[b]}$ is an injective group homomorphism.

For $\tau \in \mathfrak{S}_b$ and $r \in [1,s]$, define $\tau[r] \in \mathfrak{S}_{sb}$ by

$$((i-1)b + j)\ \tau[r] = \begin{cases} (r-1)b + j\tau, & \text{if } i = r,\\ (i-1)b + j, & \text{otherwise,} \end{cases}$$

for all $i \in [1,s]$ and $j \in [1,b]$, so that $\tau[r]$ acts on the r-th successive block of size b in $[1,sb]$ according to τ, and fixes everything else. Note that as a permutation on the set $((r-1)b, rb]$, $\tau[r]$ is independent of s (as long as $s \geq r$). As this notation also depends on b (i.e. the degree of the symmetric group in which τ lies), we will specify b when it is unclear from the context what b is.

In addition, define $\Delta_a\tau \in \mathfrak{S}_{ab}$ by $\Delta_a\tau = \prod_{i=1}^{a} \tau[i]$, so that $\Delta_a\tau$ permutes each of the a successive blocks of size b in $[1,ab]$ simultaneously according to τ. Clearly, the maps $\tau \mapsto \tau[r]$ and $\tau \mapsto \Delta_a\tau$ are injective group homomorphisms.

If $H \subseteq \mathfrak{S}_a$, $K \subseteq \mathfrak{S}_b$ and $r \in \mathbb{Z}^+$, we write

$$\begin{aligned}
H^{[b]} &= \{h^{[b]} \mid h \in H\},\\
K[r] &= \{k[r] \mid k \in K\},\\
\Delta_a K &= \{\Delta_a k \mid k \in K\}.
\end{aligned}$$

We note the following lemma, whose proof is straightforward.

Lemma 2.1. *Let $\sigma \in \mathfrak{S}_a$ and $\tau \in \mathfrak{S}_b$.*

(1) *If* $r \in [1, a]$, *then* $\tau[r]^{\sigma^{[b]}} = \tau[r\sigma]$.
(2) $\sigma^{[b]}(\Delta_a \tau) = (\Delta_a \tau)\sigma^{[b]}$.

Assume $n = pk$. Given a set partition of $[1, n]$ into k blocks of size p, we have a subgroup D of $\mathfrak{S}_n$ which is isomorphic to $\mathfrak{S}_p \times \mathfrak{S}_k$ where each factor acts regularly: the factor $\mathfrak{S}_k$ permutes the k blocks according to $\mathfrak{S}_k$, while the factor $\mathfrak{S}_p$ act on each of the k blocks simultaneously, and these two actions commute. Any two such groups arising from two set partitions are conjugate in $\mathfrak{S}_n$.

Such a group D can be viewed as a subgroup of a wreath product $\mathfrak{S}_p \wr \mathfrak{S}_k$: let $\mathfrak{S}_k^{[p]}$ be the fixed top group; its centralizer in the base group is the diagonal product $\Delta_k \mathfrak{S}_p$ which is isomorphic to $\mathfrak{S}_p$, and then one can take $D = \Delta_k \mathfrak{S}_p \times \mathfrak{S}_k^{[p]}$.

3. The problem

Assume F is a field of characteristic p, and let $k \in \mathbb{Z}^+$ with $p \nmid k$ and let $n = pk$. In [ES, §4], the module $\mathrm{Lie}(n)$ is studied via a different module, called the p-th symmetrisation of $\mathrm{Lie}(k)$, denoted by $S^p(\mathrm{Lie}(k))$; we will give a precise definition below. This module is related to $\mathrm{Lie}(n)$ as follows.

Theorem 3.1. [ES, Theorem 10] *Assume $n = pk$ where p does not divide k. Then there is a short exact sequence of right $F\mathfrak{S}_n$-modules*

$$0 \to \mathrm{Lie}(n) \to eF\mathfrak{S}_n \to S^p(\mathrm{Lie}(k)) \to 0$$

where e is an idempotent in $\mathfrak{S}_n$.

As a corollary, we see that $\Omega(S^p(\mathrm{Lie}(k))) \cong \mathrm{Lie}(n)_{pf}$ (where here, and hereafter, Ω is the Heller operator, taking a module to the kernel of its projective cover).

To define $S^p(\mathrm{Lie}(k))$, take the regular subgroup $D = \Delta_k(\mathfrak{S}_p) \times \mathfrak{S}_k^{[p]}$ as described at the end of §2. Let Λ_k be the outer tensor product $\Lambda_k = F \boxtimes \mathrm{Lie}(k)$, and take $S^p(\mathrm{Lie}(k)) \cong \mathrm{Ind}_D^{\mathfrak{S}_n} \Lambda_k$. [The module is the same as that given in [ES]]. The action of $\Delta_k \mathfrak{S}_p$ on Λ_k is trivial, while that of $\mathfrak{S}_k^{[p]}$ on Λ_k is equivalent to that of $\mathfrak{S}_k$ on $\mathrm{Lie}(k)$.

Let P be a fixed Sylow p-subgroup of $\mathfrak{S}_n$. By Mackey's formula, we have

$$\mathrm{Res}_P^{\mathfrak{S}_n} S^p(\mathrm{Lie}(k)) \cong \mathrm{Res}_P^{\mathfrak{S}_n} \mathrm{Ind}_D^{\mathfrak{S}_n} \Lambda_k = \bigoplus_{x \in D/\mathfrak{S}_n \backslash P} \mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x).$$

Proposition 3.2.

(1) *If* $(\Delta_k \mathfrak{S}_p)^x \cap P = 1$, *then* $\mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)$ *is projective.*
(2) *If* $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, *then* $\mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)$ *has no projective summand.*

Proof. If $(\Delta_k \mathfrak{S}_p)^x \cap P = 1$, then $\Delta_k \mathfrak{S}_p \cap P^{x^{-1}} = 1$; we claim that in this case $\mathrm{Res}_{D \cap P^{x^{-1}}} \Lambda_k$ is projective, so that (1) follows.

To prove the claim, let $Q = D \cap P^{x^{-1}}$, then $\Delta_k \mathfrak{S}_p \cap Q = 1$. If R is a Sylow p-subgroup of $\Delta_k \mathfrak{S}_p$, then all D-conjugates of R lie in $\Delta_k \mathfrak{S}_p$, since $\Delta_k \mathfrak{S}_p$ is normal in D; thus $R^d \cap Q = 1$ for all $d \in D$. Now, Λ_k is by construction relatively R-projective, so that Λ_k is a direct summand of $\mathrm{Ind}_R^D U$ for some R-module U. It follows that $\mathrm{Res}_Q \Lambda_k$ is a direct summand of $\mathrm{Res}_Q \mathrm{Ind}_R^D U$. But by Mackey's formula, $\mathrm{Res}_Q \mathrm{Ind}_R^D U = \bigoplus_{d \in R/D \backslash Q} \mathrm{Ind}_{R^d \cap Q}^Q (U \otimes x)$. Since $R^d \cap Q = 1$, each summand $\mathrm{Ind}_{R^d \cap Q}^Q (U \otimes x)$ is projective. Thus, $\mathrm{Res}_Q \mathrm{Ind}_R^D U$ and $\mathrm{Res}_Q \Lambda_k$ are projective.

If $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, let $\sigma \in \mathfrak{S}_p$ such that $(\Delta_k \sigma)^x \in (\Delta_k \mathfrak{S}_p)^x \cap P$. Then since $\Delta_k \sigma$ acts trivially on the entire module Λ_k, we see that $\mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)$ cannot have any projective summand. □

In view of Proposition 3.2, let S be the set of all double coset representatives in $D/\mathfrak{S}_n \setminus P$ such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. Then we have

Corollary 3.3. *Assume $n = pk$ with $p \nmid k$. Then*

$$(\mathrm{Res}_P^{\mathfrak{S}_n} S^p(\mathrm{Lie}(k)))_{pf} \cong \bigoplus_{x \in S} \mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x).$$

The following identifies the Ω-translate of this module.

Lemma 3.4. *For $x \in S$ we have*

$$\Omega(\mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)) \cong \mathrm{Ind}_{D^x \cap P}^P ((\Omega(F) \boxtimes \mathrm{Lie}(k)) \otimes x),$$

and $\Omega(F)$ has dimension $p - 1$.

Proof. Recall that $\Lambda_k \cong F \boxtimes \mathrm{Lie}(k)$. Since $\mathrm{Lie}(k)$ is a projective $F\mathfrak{S}_k$-module, we see that $\Omega(\Lambda_k) \cong \Omega(F) \boxtimes \mathrm{Lie}(k)$. Furthermore, $\Omega(F)$ can be described as follows: the natural p-dimensional permutation module of $F\mathfrak{S}_p$ is indecomposable projective and has F as a quotient, so that $\Omega(F)$ is its maximal submodule, of dimension $(p-1)$. Moreover, $\Omega(F)$ remains indecomposable when restricted to any subgroup of $\mathfrak{S}_p$ of order p. Now, the short exact sequence

$$0 \to \Omega(F) \boxtimes \mathrm{Lie}(k) \to P(\Lambda_k) \to \Lambda_k \to 0,$$

where $P(\Lambda_k)$ denotes the projective cover of Λ_k, gives the following short exact sequence

$$(*) \quad 0 \to \mathrm{Ind}_{D^x \cap P}^P ((\Omega(F) \boxtimes \mathrm{Lie}(k)) \otimes x) \to \mathrm{Ind}_{D^x \cap P}^P (P(\Lambda_k) \otimes x) \to \mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x) \to 0.$$

Let $1 \neq \sigma \in \mathfrak{S}_p$ such that $(\Delta_k \sigma)^x \in (\Delta_k \mathfrak{S}_p)^x \cap P$. Then $(\Delta_k \sigma)^x$ acts trivially on $\mathrm{Lie}(k)$, and $\Omega(F)$ is indecomposable as a module for $\langle \Delta_k \sigma \rangle$ (as $\Delta_k \sigma$ has order p) and has dimension $(p-1)$. It follows that $\mathrm{Ind}_{D^x \cap P}^P ((\Omega(F) \boxtimes \mathrm{Lie}(k)) \otimes x)$ has no projective summand. Thus, from $(*)$, we see that

$$\Omega(\mathrm{Ind}_{D^x \cap P}^P (\Lambda_k \otimes x)) \cong \mathrm{Ind}_{D^x \cap P}^P ((\Omega(F) \boxtimes \mathrm{Lie}(k)) \otimes x)$$

since $\mathrm{Ind}_{D^x \cap P}^P(P(\Lambda_k) \otimes x)$ is projective. □

The following is the main result of this section.

Theorem 3.5. *Assume $n = pk$ with $p \nmid k$. We have*

$$\dim((\mathrm{Res}_P^{\mathfrak{S}_n} \mathrm{Lie}(n))_{pf}) = (p-1)(k-1)! \sum_{x \in S} [P : D^x \cap P].$$

Proof. Restriction is exact, hence we have a short exact sequence

$$0 \to \mathrm{Res}_P \mathrm{Lie}(n) \to \mathrm{Res}_P(eF\mathfrak{S}_n) \to \mathrm{Res}_P S^p(\mathrm{Lie}(k)) \to 0.$$

Since $\mathrm{Res}_P(eF\mathfrak{S}_n)$ remains projective as an FP-module, we see that

$$(\mathrm{Res}_P \mathrm{Lie}(n))_{pf} \cong \Omega(\mathrm{Res}_P S^p(\mathrm{Lie}(k)) \cong \bigoplus_{x \in S} \Omega(\mathrm{Ind}_{D^x \cap P}^P(\Lambda_k \otimes x))$$

by Corollary 3.3. Now, by 3.4, we have $\Omega(\mathrm{Ind}_{D^x \cap P}^P(\Lambda_k \otimes x))$ for $x \in S$ is isomorphic to $\mathrm{Ind}_{D^x \cap P}^P((\Omega(F) \boxtimes \mathrm{Lie}(k)) \otimes x)$ and that $\Omega(F)$ has dimension $p-1$. This proves the Theorem. □

Corollary 3.6. *We have*

$$\dim((\mathrm{Res}_P^{\mathfrak{S}_{kp}} \mathrm{Lie}(kp))_{pf}) = (p-1)(k-1)!N,$$

where N is the number of cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$.

Proof. Using Theorem 3.5 we must show that $N = N'$ where $N' = \sum_{y \in S} [P : D^y \cap P]$. The index $[P : D^y \cap P]$ is equal to the size of the P-orbit of Dy in the coset space $(\mathfrak{S}_n : D)$, so it is equal to the number of cosets Dx contained in DyP.

Write $D_1 = \Delta_k \mathfrak{S}_p$. If a coset Dx is contained in DyP then $D_1^x \cap P$ is P-conjugate to $D_1^y \cap P$ and hence $D_1^y \cap P \neq 1$ if and only if $D_1^x \cap P \neq 1$. Conversely if Dx is a coset and $D_1^x \cap P \neq 1$ then Dx is contained in one of the double cosets counted for N'. We sum over all such double cosets, and hence $N = N'$. □

Corollary 3.6 suggests that we should proceed by parametrising the right cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. When $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, this is a non-trivial p-subgroup of P conjugate to a subgroup of $\Delta_k \mathfrak{S}_p$, and hence it is generated by an element $y \in P$ of order p which is fixed-point-free as an element of $\mathfrak{S}_{kp}$. We shall study these elements in the next section.

4. Sylow p-subgroups of symmetric groups

We analyze the Sylow p-subgroups of symmetric groups, especially its fixed-point-free elements of order p, in this section. In order to exploit the orbit structure of such elements, we make the following definitions.

Definition 4.1. Let $n \in \mathbb{Z}^+$.

(1) A *partition* of the interval $(0, n]$ is an increasingly ordered subset $\{a_0, \ldots, a_s\}$ of $(0, n]$ with $a_0 = 0$ and $a_s = n$.

(2) A partition $\{b_0, \dots, b_t\}$ of $(0, n]$ is *finer* than $\{a_0, \dots, a_s\}$ provided for each $r \in [1, s]$, there exists $j_r \in [1, t]$ such that $a_r = b_{j_r}$.
(3) Let $\sigma \in \mathfrak{S}_n$. The partition $\{a_0, \dots, a_s\}$ of $(0, n]$ is *σ-invariant* provided for each $r \in [1, s]$, the subinterval $(a_{r-1}, a_r]$ is σ-invariant, that is $\sigma(a_{r-1}, a_r] = (a_{r-1}, a_r]$.

Lemma 4.2. *Let $\sigma \in \mathfrak{S}_n$. There is a unique finest σ-invariant partition of the interval $(0.n]$.*

We may thus speak of *the* finest σ-invariant partition of $(0, n]$, which is finer than every other σ-invariant partition of $(0, n]$. We leave the proof of the Lemma to the reader.

The Sylow p-subgroups of $\mathfrak{S}_n$ are direct products of iterated wreath products of cyclic groups of order p. We proceed with the analysis of these building blocks.

From now on, we denote the distinguished p-cycle $(1, 2, \dots, p)$ by π.

Definition 4.3.

(1) For each $i \in \mathbb{Z}_{\geq 0}$, let R_i be the subgroup of $\mathfrak{S}_{p^{i+1}}$ generated by $\{\pi^{[p^j]} \mid j \in [0, i]\}$. Then R_i is a Sylow p-subgroup of $\mathfrak{S}_{p^{i+1}}$. For convenience, let $\pi^{[p^{-1}]} = 1$, and $R_{-1} = 1$.
(2) For each $i \in \mathbb{Z}_{\geq 0}$, let $B_i = R_{i-1}[1] \times R_{i-1}[2] \times \cdots \times R_{i-1}[p]$. For convenience, let $B_{-1} = \emptyset$.
(3) And for each $s \in \mathbb{Z}^+$, let $H_s = \prod_{a=1}^{s} \langle \pi[a] \rangle$.

Note. For each $i \in \mathbb{Z}_{\geq 0}$ we have $R_i = B_i \rtimes \langle \pi^{[p^i]} \rangle$, and, as a group, R_i is isomorphic to $\underbrace{C_p \wr C_p \wr \cdots \wr C_p}_{(i+1)\text{ times}}$. Also, H_{p^i} is a subgroup of B_i, and it is normal in R_i.

The finest g-invariant partition of the interval $(0, p^{i+1}]$ for $g \in R_i$ has nice properties:

Proposition 4.4. *Suppose that $g \in R_i$, and let $\{a_0 < a_1 < \cdots < a_s\}$ be the finest g-invariant partition of the interval $(0, p^{i+1}]$. Then*

(1) *$a_j - a_{j-1}$ is a power of p, dividing a_j, for all $1 \leq j \leq s$;*
(2) *$g = \prod_{j=1}^{s} \gamma_j[a_j/p^{\lambda_j}]$ where $a_j - a_{j-1} = p^{\lambda_j}$, with $\gamma_j \in R_{\lambda_j - 1} \setminus B_{\lambda_j - 1}$ for all $1 \leq j \leq s$.*

Note that the factor $\gamma_j[a_j/p^{\lambda_j}]$ appearing in Proposition 4.4(2) is just γ_j with its support translated from $(0, p^{\lambda_j}]$ $(= (0, a_j - a_{j-1}])$ to $(a_{j-1}, a_j]$.

Proof. We prove the first two statements by induction on i. When $i = 0$, either $g = 1$, in which case $s = p$ and $a_j = j$ for all $0 \leq j \leq s$, or else $g = \pi^t$ for some $t \in \mathbb{Z}_p^*$, in which case $s = 1$ and so $a_1 = p$. It can easily be checked that both statements hold in either case.

Assume now $i > 0$. The statements are trivial when $s = 1$. When $s > 1$, we have $g \in B_i$. Thus, $g = \prod_{j=1}^{p} g_j[j]$ for some $g_1, g_2, \dots, g_p \in R_{i-1}$, so that $\{0, p^i, 2p^i, \dots, p^{i+1}\}$ is a g-invariant partition of $(0, p^{i+1}]$. Hence by Lemma

4.2, there exist $j_1, \dots, j_p \in [1, s]$ such that $a_{j_r} = rp^i$ for $r \in [1, p]$. Now the partition $\{a_{j_{r-1}}, \dots, a_{j_r}\}$ of the interval $((r-1)p^i, rp^i]$ must be the finest g_r-invariant partition of $(0, p^i]$ linearly translated by $(r-1)p^i$. Induction hypothesis applied to g_r then yields for each $j \in (j_{r-1}, j_r]$, $a_j - a_{j-1}$ is a power of p, say p^{λ_j}, dividing $a_j - (r-1)p^i$. Since $p^{\lambda_j} = a_j - a_{j-1} \le p^i$, we see that $\lambda_j \le i$, and so p^{λ^j} divides $(a_j - (r-1)p^i) + (r-1)p^i = a_j$. Also by induction, g_r is a product of $\gamma_j \in R_{\lambda_j - 1} \setminus B_{\lambda_j - 1}$ whose support is translated from $(0, p^{\lambda_j}]$ to $(a_{j-1} - (r-1)p^i, a_j - (r-1)p^i]$. Thus $g_r[r]$ is a product of γ_j whose support is translated from $(0, p^{\lambda_j}]$ to $(a_{j-1}, a_j]$, and the proof is complete. □

For $g \in R_i$ of order p and is fixed-point-free as an element of $\mathfrak{S}_{p^{i+1}}$, the λ_j's appearing in Proposition 4.4(2) are all positive. Furthermore, each γ_j is conjugate to a unique power of $\pi^{[p^i]}$; we present below a proof of this, in a more general setting.

Proposition 4.5. *Let G be a group of the form $G = R \wr \langle y \rangle$ where y has order p, with base group B. Let $t \in \mathbb{Z}_p^*$. Then the conjugacy class of y^t contains precisely the elements of G having order p and lying in the coset By^t.*

Thus, the elements of $G \setminus B$ having order p are just the various conjugates of y^t for $t \in \mathbb{Z}_p^*$.

Proof. It suffices to prove the proposition for $t = 1$ since y^t also generates the group $\langle y \rangle$. Let C be the conjugacy class of y, and let $\Gamma = \{g \in By \mid g$ has order $p\}$. It is easy to see that $C \subseteq \Gamma$. For the converse, we show that every element of Γ is conjugate to y by a unique element of B', where B' is the direct product of $p-1$ copies of R, say $B' = R \times \cdots \times R \times 1 \subseteq B$. Let $g = by \in \Gamma$, where $b \in B$. Then $g^p = b({}^y b)({}^{y^2} b) \cdots ({}^{y^{p-1}} b)$ (where ${}^x b = xbx^{-1}$). If $b = (r_1, \dots, r_p)$ then the coordinates of g^p are the cyclic permutations of $r_1 r_2 \dots r_p$. Hence $g^p = 1$ if and only if $r_p = (r_1 r_2 \dots r_{p-1})^{-1}$. This shows that given $r_1, \dots, r_{p-1} \in R$ there is a unique such g of order p. Hence $|\Gamma| \le |R|^{p-1}$. The set $A := \{(b')^{-1} y b' : b' \in B'\}$ is contained in Γ, and has size $|B'| = |R|^{p-1}$ since the centraliser of y in B' is trivial. It follows that $A = \Gamma$, and $g = (b')^{-1} y b'$ for a unique $b' \in B'$, and the proof is complete. □

Corollary 4.6 (of proof)**.** *Every element of $R_i \setminus B_i$ having order p can be uniquely expressed as $((\pi^{[p^i]})^t)^b$ with $b \in \prod_{j=1}^{p-1} R_{i-1}[j]$ and $t \in \mathbb{Z}_p^*$.*

Take $g \in R_i$. We have seen in Proposition 4.4(1) that if $\{a_0, \dots, a_s\}$ is finest g-invariant partition of $(0, p^{i+1}]$, then $a_j - a_{j-1}$ are p-powers, dividing a_j. Clearly, these p-powers, or more simply their exponents, completely determines the finest g-invariant partition. This suggests the following terminology.

Definition 4.7. A *p-composition* $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ is a finite sequence of non-negative integers such that for each $j \in [1, s]$, the partial sum $\sum_{i=1}^{j} p^{\lambda_i}$ is divisible by p^{λ_j}.

Let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ be a p-composition. For each $j \in [1, s]$, we will denote these partial sums in the following by

$$\Sigma_j^\lambda := \sum_{i=1}^{j} p^{\lambda_i}.$$

If $\sum_{i=1}^{s} p^{\lambda_i} = r$, we say that λ is a *p-composition of r*.

Clearly, if $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ is a p-composition, then $\{0, \Sigma_1^\lambda, \Sigma_2^\lambda, \ldots, \Sigma_s^\lambda\}$ is a partition of the interval $(0, \Sigma_s^\lambda]$.

Proposition 4.8. *Let $g \in R_i$, and let $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$, where λ_i's are as in Proposition 4.4(2). Then λ is a p-composition of p^{i+1}.*

Conversely, every p-composition of p^{i+1} arises in this way. More precisely, if $\mu = (\mu_1, \ldots, \mu_t)$ is a p-composition of p^{i+1}, then $\{0, \Sigma_1^\mu, \ldots, \Sigma_t^\mu\}$ is the finest g-invariant partition of the interval $(0, p^{i+1}]$, where

$$g := \prod_{r=1}^{t} \pi^{[p^{\mu_r - 1}]}[\Sigma_r^\mu / p^{\mu_r}] \in R_i.$$

Proof. The first assertion follows immediately from Proposition 4.4, while the second can be verified easily. $\square$

An important p-composition is defined as follows.

Definition 4.9. Let $r \in \mathbb{Z}^+$, and let $r = \sum_{i=0}^{t} b_i p^i$ be its p-adic expansion, with $b_t \neq 0$. The p-composition $(t^{b_t}, (t-1)^{b_{t-1}}, \ldots, 0^{b_0})$ with b_t parts equal to t, b_{t-1} parts equal to $t-1$, and so on, is called the *p-adic p-composition of r*.

Lemma 4.10.

(1) *Let γ be a p-composition of ap^m for some $a \in \mathbb{Z}^+$, and let δ be a p-composition of p^j with $j \leq m$. Then the concatenation (γ, δ) is a p-composition.*
(2) *If $\lambda = (\lambda_1, \ldots, \lambda_s)$ is a p-composition, and $\mu^{(i)}$ is a p-composition of p^{λ_i} for all $1 \leq i \leq s$, then the concatenation $\mu := (\mu^{(1)}, \mu^{(2)}, \ldots, \mu^{(s)})$ is a p-composition.*

Proof. For part (1), if δ_i is a part of δ then $\delta_i \leq j \leq m$ and therefore p^{δ_i} divides ap^m. Since p^{δ_i} also divides Σ_i^δ (as δ is a p-composition), it divides $ap^m + \Sigma_i^\delta$. Thus (γ, δ) is a p-composition. Part (2) follows by induction and part (1). $\square$

Definition 4.11. Suppose that λ, μ are as in Lemma 4.10(2). Then we say that μ is a *refinement* of λ.

Corollary 4.12. *Let λ be a p-composition of p^m with more than one part. Then λ is a refinement of the p-composition $((m-1)^p)$.*

Proof. By Proposition 4.8, λ arises from the finest g-invariant partition $\mathcal{P}$ of the interval $(0, p^m]$ for some $g \in R_{m-1}$. Since λ has more than one part, so

does $\mathcal{P}$. Thus $g \in B_{m-1}$, so that $\{0, p^{m-1}, 2p^{m-1}, \dots, p^m\}$ is a g-invariant partition of $(0, p^m]$. Hence $\mathcal{P}$ is finer than $\{0, p^{m-1}, 2p^{m-1}, \dots, p^m\}$, and in turn, λ is a refinement of $((m-1)^p)$. □

Recall that R_i is an explicit Sylow p-subgroup of $\mathfrak{S}_{p^{i+1}}$, with support $(0, p^{i+1}]$. We will now fix an explicit Sylow p-subgroup of $\mathfrak{S}_{pk}$. Let $\kappa = (\kappa_1, \dots, \kappa_l)$ be the p-adic p-composition of k. Then $(0, p\Sigma_1^\kappa, \dots, p\Sigma_l^\kappa]$ is a partition of the interval $(0, pk]$. We choose our Sylow p-subgroup to be the product of R_{κ_i} whose support is translated from $(0, p^{\kappa_i+1}]$ to $(p\Sigma_{i-1}^\kappa, p\Sigma_i^\kappa]$.

The following gives the precise description of this choice in general.

Definition 4.13. Let $\kappa = (\kappa_1, \kappa_2, \dots, \kappa_l)$ be the p-adic p-composition of k, and let P_k be the Sylow p-subgroup of $\mathfrak{S}_{pk}$ chosen as follows:

$$P_k = P_k(1) \times P_k(2) \times \cdots \times P_k(l),$$

where $P_k(i) = R_{\kappa_i}[\Sigma_i^\kappa / p^{\kappa_i}]$ for all i. That is, the i-th factor $P_k(i)$ is a copy of R_{κ_i} with support being translated from $(0, p^{\kappa_i+1}]$ to $(p\Sigma_{i-1}^\kappa, p\Sigma_i^\kappa]$.

Note. Note that $\pi^{[p^i]}[j] \in P_k$ if and only if $jp^i \leq k$. In fact,

$$P_k = \langle \pi^{[p^i]}[j] \mid jp^i \leq k \rangle.$$

This may be used as an alternative definition of P_k.

Notation 4.14. In what follows, we will frequently have expressions of the form $\prod_{i=1}^l x_i[\Sigma_i^\kappa / p^{\kappa_i}]$ and $\prod_{i=1}^l A_i[\Sigma_i^\kappa / p^{\kappa_i}]$ where for each $i \in [1, l]$, x_i and A_i are respectively an element and a subset of $\mathfrak{S}_{p^{\kappa_i+1}}$. Most of the time, the details of the shifts do not play a role. We will therefore use the shorthand notations

$$\prod_\kappa x_i \quad \text{and} \quad \prod_\kappa A_i$$

to denote these expressions.

Similarly if $\lambda = (\lambda_1, \dots, \lambda_s)$ is a p-composition then we write

$$\prod_\lambda x_i = \prod_{i=1}^s x_i[\Sigma_i^\lambda / p^{\lambda_i}]$$

(where $x_i \in \mathfrak{S}_{p^{\lambda_i+1}}$).

Lemma 4.15. *Let P_k be the Sylow p-subgroup of $\mathfrak{S}_{kp}$ defined above. Then we have $P_k \subseteq P_{k+1}$.*

Proof. This follows from the fact that $P_k = \langle \pi^{[p^i]}[j] \mid jp^i \leq k \rangle$. □

For each $g \in P_k$, we have $g = \prod_\kappa \rho_i$ for some $\rho_i \in R_{\kappa_i}$ for all $i \in [1, l]$. By Proposition 4.4, each ρ_i is associated with a p-composition $\lambda^{(i)}$ of p^{κ_i+1} arising from the finest ρ_i-invariant partition of the interval $(0, p^{\kappa_i+1}]$. The concatenation λ of these p-compositions is again a p-composition, of pk, by Lemma 4.10 (note that $(\kappa_1+1, \kappa_2+1, \dots, \kappa_l+1)$ is the p-adic p-composition of pk).

If in addition g is fixed-point-free as an element of $\mathfrak{S}_{pk}$, then the parts in each $\lambda^{(i)}$ are positive. Subtracting each part in $\lambda^{(i)}$ by 1 produces a

p-composition $\bar{\lambda}^{(i)}$ of p^{κ_i}, and the concatenation $\bar{\lambda}$ of these $\bar{\lambda}^{(i)}$ is a p-composition of k. We call $\bar{\lambda}$ the p-composition of k associated to the fixed-point-free element g of P_k.

The following shows that every p-composition of k arises in this way. In fact, each is associated to some fixed-point-free element g of P_k of order p.

Proposition 4.16. *Let $k \in \mathbb{Z}^+$, and let $\lambda = (\lambda_1, \dots, \lambda_s)$ be a p-composition of k. Then λ is associated to some fixed-point-free element $g \in P_k$ of order p.*

Proof. If $s = 1$, then we apply Proposition 4.8. So suppose $s > 1$ and let $r = \Sigma^{\lambda}_{s-1}$ $(= k - p^{\lambda_s})$. By induction $(\lambda_1, \dots, \lambda_{s-1})$ is associated to some $g_1 \in P_r$ of order p which is fixed-point-free on $(0, pr]$. Since $\pi^{[p^{\lambda_s}]}[k/p^{\lambda_s}] \in P_k$, is transitive and fixed-point-free on $(pr, pk]$, we see that $g = g_1 \pi^{[p^{\lambda_s}]}[k/p^{\lambda_s}] \in P_k$ has order p, is fixed-point-free on $(0, pk]$, with associated p-composition λ. □

Proposition 4.17. *Let $k \in \mathbb{Z}^+$, with p-adic p-composition $\kappa = (\kappa_1, \dots, \kappa_l)$. Then every p-composition of k is a refinement of κ.*

Proof. Let $\lambda = (\lambda_1, \dots, \lambda_s)$ be a p-composition of k. By Proposition 4.16, λ is associated to a fixed-point-free element $g \in P_k$ of order p. Equivalently, $\{0, p\Sigma^{\lambda}_1, p\Sigma^{\lambda}_2, \dots, p\Sigma^{\lambda}_s\}$ is the finest g-invariant partition of the interval $(0, pk]$. But since $P_k \subseteq \prod_\kappa \mathfrak{S}_{p^{\kappa_i+1}}$, we see that $\{0, p\Sigma^{\kappa}_1, p\Sigma^{\kappa}_2, \dots, p\Sigma^{\kappa}_l\}$ is a g-invariant partition of the interval $(0, pk]$. Thus, $\{0, p\Sigma^{\lambda}_1, p\Sigma^{\lambda}_2, \dots, p\Sigma^{\lambda}_s\}$ is finer than $\{0, p\Sigma^{\kappa}_1, p\Sigma^{\kappa}_2, \dots, p\Sigma^{\kappa}_l\}$, and hence $\{0, \Sigma^{\lambda}_1, \Sigma^{\lambda}_2, \dots, \Sigma^{\lambda}_s\}$ is finer than $\{0, \Sigma^{\kappa}_1, \Sigma^{\kappa}_2, \dots, \Sigma^{\kappa}_l\}$, which in turn shows that λ is a refinement of κ. □

5. Finding right coset representatives

We will now analyse the right cosets Dx such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$; from now on, $P = P_k$, as defined in Definition 4.13. Our aim in this section is to find a good subset $X_k \subseteq \mathfrak{S}_{pk}$ such that

- $(\Delta_k \mathfrak{S}_p)^y \cap P \neq 1$ for all $y \in X_k$;
- if $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, then there exists $y \in X_k$ such that $Dx = Dy$.

When $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$, this is a non-trivial p-subgroup of P conjugate to a subgroup of $\Delta_k \mathfrak{S}_p$, and hence it is generated by a fixed-point-free element y of P of order p. Clearly we can replace x by elements of the form dx with $d \in D$ without altering the right coset Dx. Taking d suitably in $\Delta_k \mathfrak{S}_p \subseteq D$ will allow us to have $y = (\Delta_k \pi)^x$ in P. Such x takes orbits of $\Delta_k \pi$ to orbits of y, and the order in which these orbits appear can be controlled by modifying with $d \in \mathfrak{S}^{[p]}_k$. The following makes this precise.

Proposition 5.1. *Let κ and P be as in Definition 4.13. Let $x \in \mathfrak{S}_{pk}$ such that $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$. Then for each $r \in [1, l]$ there exists $x_r \in \mathfrak{S}_{p^{\kappa_r+1}}$ such that*

- $\prod_\kappa x_j \in Dx$;
- $(\Delta_{p^{\kappa_r}} \pi)^{x_r} \in R_{\kappa_r}$.

Proof. Let $1 \neq y \in (\Delta_k \mathfrak{S}_p)^x \cap P$, say $y = (\Delta_k g)^x$ for some p-cycle $g \in \mathfrak{S}_p$. Then $g = \pi^\tau$ for some $\tau \in \mathfrak{S}_p$; and by replacing x with $(\Delta_k \tau)x \in Dx$ we may assume $g = \pi$.

Since $y \in P = P(1) \times \cdots \times P(l)$, we have $y = \prod_{r=1}^{l} y_r$ where for each r, $y_r \in P(r) = R_{\kappa_r}[\Sigma_r^\kappa / p^{\kappa_r}]$. As $\prod_{r=1}^{l} y_r = (\Delta_k \pi)^x = \prod_{i=1}^{k} (\pi[i])^x$, there exists $\sigma \in \mathfrak{S}_k$ permuting the cycles of $\Delta_k \pi$ such that, for each $r \in [1, l]$, we have $\prod_{i=\Sigma_{r-1}^\kappa+1}^{\Sigma_r^\kappa} \pi[i\sigma]^x = y_r$. Recall that $\prod_{i=1}^{k} \pi[i\sigma] = (\Delta_k \pi)^{\sigma^{[p]}}$, so by replacing x with $\sigma^{[p]} x \in Dx$, we may assume that

$$((\Delta_{p^{\kappa_r}} \pi)[\Sigma_r^\kappa / p^{\kappa_r}])^x = y_r \in P(r) = R_{\kappa_r}[\Sigma_r^\kappa / p^{\kappa_r}]$$

for all $r \in [1, l]$. Thus x preserves the orbits of P and we can write $x = \prod_{r=1}^{l} z_r$, where $z_r \in \mathfrak{S}_{p^{\kappa_r+1}}[\Sigma_r^\kappa / p^{\kappa_r}]$ for all r, and $y_r = ((\Delta_{p^{\kappa_r}} \pi)[\Sigma_r^\kappa / p^{\kappa_r}])^{z_r}$. The proposition follows by defining x_r to be the element of $\mathfrak{S}_{p^{\kappa_r+1}}$ such that $x_r[\Sigma_r^\kappa / p^{\kappa_r}] = z_r$. ☐

This shows in particular that we can take x so that it respects the direct factors of P. We have the following refinement, which concentrates on a fixed factor of P. The proof is analogous to that of Proposition 5.1.

Proposition 5.2. *Suppose that $(\Delta_{p^m} \pi)^x \in R_m$ for some $x \in \mathfrak{S}_{p^{m+1}}$. Then there exist a p-composition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ of p^m, and elements $x_r \in \mathfrak{S}_{p^{\lambda_r+1}}$ for all $r \in [1, s]$ such that*

- $\prod_\lambda x_r \in \mathfrak{S}_{p^m}^{[p]} x$;
- $(\Delta_{p^{\lambda_r}} \pi)^{x_r} \in R_{\lambda_r} \setminus B_{\lambda_r}$.

Proof. By Proposition 4.4 and Proposition 4.8, there exist a p-composition $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_s)$ of p^m, and elements $\gamma_r \in R_{\lambda_r} \setminus B_{\lambda_r}$ for $r \in [1, s]$, such that $(\Delta_{p^m} \pi)^x = \prod_\lambda \gamma_r$. Thus there is some $\sigma \in \mathfrak{S}_{p^m}$ such that $(\prod_{i=\Sigma_{r-1}^\lambda+1}^{\Sigma_r^\lambda} \pi[i\sigma])^x = \gamma_r[\Sigma_r^\lambda / p^{\lambda_r}]$ for all $r \in [1, s]$. By replacing x by $\sigma^{[p]} x \in \mathfrak{S}_{p^m}^{[p]} x$, we may assume that

$$((\Delta_{p^{\lambda_r}} \pi)[\Sigma_r^\lambda / p^{\lambda_r}])^x = \gamma_r[\Sigma_r^\lambda / p^{\lambda_r}]$$

for all r. Thus $x = \prod_{r=1}^{s} z_r$, where $z_r \in \mathfrak{S}_{p^{\lambda_r+1}}[\Sigma_r^\lambda / p^{\lambda_r}]$, and

$$\gamma_r[\Sigma_r^\lambda / p^{\lambda_r}] = ((\Delta_{p^\lambda} \pi)[\Sigma_r^\lambda / p^{\lambda_r}])^{z_r}.$$

The Proposition follows by defining x_r to be the element of $\mathfrak{S}_{p^{\lambda_r+1}}$ such that $x_r[\Sigma_r^\lambda / p^{\lambda_r}] = z_r$. ☐

We now find good coset representatives for these x_r, and we start by defining distinguished elements which will conjugate $\Delta_{p^m} \pi$ to $(\pi^{[p^m]})^t$.

Definition 5.3. For $t \in \mathbb{Z}_p^*$ and $m \in \mathbb{Z}_{\geq 0}$, define $z_{m,t} \in \mathfrak{S}_{p^{m+1}}$ by

$$((i-1)p + j) z_{m,t} := i + (\overline{t(j-1)}) p^m \quad (i \leq p^m, j \leq p).$$

Here, and hereafter, given an integer x, we write $\overline{x}$ for the residue of x (mod p) with $0 \leq \overline{x} < p$.

For example, if $m = 0$ then $z_{0,t}$ normalizes the group $\langle \pi \rangle$ (see Lemma 5.4 below), and $z_{0,1} = 1$.

Note. It will be convenient to describe $z_{m,t}$ by making use of the natural faithful action of $\mathfrak{S}_n$ on standard tableaux. We take tableaux with p^m rows and each row of length p, i.e. of shape (p^{p^m}). Then $z_{m,1}$ is the element of $\mathfrak{S}_{p^m+1}$ which sends the tableau

$$\begin{array}{cccc} 1 & 2 & \cdots & p \\ p{+}1 & p{+}2 & \cdots & 2p \\ \vdots & \vdots & & \vdots \\ p^m{-}p{+}1 & p^m{-}p{+}2 & \cdots & p^{m+1} \end{array} \quad \text{to} \quad \begin{array}{cccc} 1 & p^m{+}1 & \cdots & (p{-}1)p^m{+}1 \\ 2 & p^m{+}2 & \cdots & (p{-}1)p^m{+}2 \\ \vdots & \vdots & & \vdots \\ p^m & 2p^m & \cdots & p^{m+1} \end{array}.$$

We denote the first tableau by T, and the second one by $\tilde{T}$, and we will use these notations later.

In general, $z_{m,t}$ sends T to the tableau

$$\begin{array}{cccc} 1 & \bar{t}p^m{+}1 & \cdots & (\overline{t(p{-}1)})p^m{+}1 \\ 2 & \bar{t}p^m{+}2 & \cdots & (\overline{t(p{-}1)})p^m{+}2 \\ \vdots & \vdots & & \vdots \\ p^m & (\bar{t}{+}1)p^m & \cdots & (\overline{t(p{-}1){+}1})p^m \end{array}$$

which is obtained from $\tilde{T}$ by permuting the columns according to $z_{0,t}$.

Lemma 5.4. *Let $z_{m,t}$ be as above.*

(1) *We have $\pi[i]^{z_{m,t}} = (i, p^m+i, \dots, (p-1)p^m+i)^t$ for $i \in [1, p^m]$. Thus, $(\Delta_{p^m}\pi)^{z_{m,t}} = (\pi^{[p^m]})^t$.*
(2) *For $s, t \in \mathbb{Z}_p^*$ we have $(\Delta_{p^m} z_{0,t}) \cdot z_{m,s} = z_{m,ts}$.*

Proof. For the first part, consider the tableaux T and $Tz_{m,t}$ above. The rows of T are the cycles of $\Delta_{p^m}\pi$, and the rows of $Tz_{m,t}$ are the cycles of $(\pi^{[p^m]})^t$. The standard formula for conjugation gives the statement. The second part follows from a direct verification using the definition of $z_{m,t}$. □

We denote by R_m^0 the subgroup of B_m consisting of elements which fix the last block of p^m elements pointwise, i.e.

$$R_m^0 = \prod_{i=1}^{p-1} R_{m-1}[i]$$

Proposition 5.5. *Suppose that $(\Delta_{p^m}\pi)^x \in R_m \setminus B_m$ for some $x \in \mathfrak{S}_{p^{m+1}}$. Then there exist unique $t \in \mathbb{Z}_p^*$, $h \in H_{p^m}$ and $b \in R_m^0$ such that*

$$hz_{m,t}b \in \mathfrak{S}_{p^m}^{[p]}\, x.$$

Proof. Since $(\Delta_{p^m}\pi)^x$ lies in $R_m \backslash B_m$ and has order p, we apply Corollary 4.6. Hence there exist unique $t \in \mathbb{Z}_p^*$ and $b \in R_m^0$ such that $(\Delta_{p^m}\pi)^x = ((\pi^{[p^m]})^t)^b$. Thus

$$(\Delta_{p^m}\pi)^x = ((\pi^{[p^m]})^t)^b = (\Delta_{p^m}\pi)^{z_{m,t}b},$$

and so $z_{m,t}bx^{-1}$ lies in the centraliser of $\Delta_{p^m}\pi$ in $\mathfrak{S}_{p^{m+1}}$, which is $H_{p^m} \rtimes \mathfrak{S}_{p^m}^{[p]}$. Hence, there exists a unique $h \in H_{p^m}$ such that $hz_{m,t}b \in \mathfrak{S}_{p^m}^{[p]}\, x$. □

Propositions 5.1, 5.2 and 5.5 suggest the following definition for the desired coset representatives.

Definition 5.6. For $m \in \mathbb{Z}_{\geq 0}$, we define the subset Y_m of $\mathfrak{S}_{p^{m+1}}$ to be

$$Y_m := \{hz_{m,t}b \mid h \in H_{p^m}, t \in \mathbb{Z}_p^*, b \in R_m^0\}$$

For example, $Y_0 = \{hz_{0,t} : h \in \langle\pi\rangle, t \in \mathbb{Z}_p^*\}$, which is the normalizer of $\langle\pi\rangle$ in $\mathfrak{S}_p$. For a p-composition $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_s)$ of d, define

$$X_\lambda := \prod_\lambda Y_{\lambda_r} \qquad \textit{and} \qquad X_d := \bigcup_\lambda X_\lambda.$$

We also have a recursive description.

Lemma 5.7.

(1) *Let $m \in \mathbb{Z}_{\geq 0}$. Then*

$$X_{p^m} = Y_m \cup \prod_{i=1}^{p} X_{p^{m-1}}[i]$$

(disjoint union, and where $X_{p^{-1}} = \emptyset$).

(2) *Let $k \in \mathbb{Z}^+$, with p-adic p-composition $\kappa = (\kappa_1, \dots, \kappa_l)$. Then*

$$X_k = \prod_\kappa X_{p^{\kappa_i}}.$$

Proof. This follows from Lemma 4.10, Corollary 4.12 and Proposition 4.17. □

We can now state the main theorem of this section.

Theorem 5.8. *Let P be as in Definition 4.13. Let $x \in \mathfrak{S}_{pk}$ such that $(\Delta_k\mathfrak{S}_p)^x \cap P \neq 1$. Then there exists $x_0 \in X_k$ such that $x_0 \in Dx$.*

Proof. This follows from Propositions 5.1, 5.2 and 5.5, and Lemma 5.7(2). □

We note that the converse of Theorem 5.8 also holds.

Lemma 5.9. *We have $(\Delta_k\mathfrak{S}_p)^y \cap P \neq 1$ for all $y \in X_k$.*

Proof. By the definition of the z_{λ_r,t_r}, the conjugate $(\Delta_k\pi)^y$ belongs to P. □

6. Uniqueness

We have seen in the previous section that $(\Delta_k\mathfrak{S}_p)^y \cap P \neq 1$ for all $y \in X_k$, and if $(\Delta_k\mathfrak{S}_p)^x \cap P \neq 1$, then there exists $x_0 \in X_k$ such that $Dx_0 = Dx$. However, x_0 need not be unique. For example, instead of x_0, one may choose $(\Delta_k\pi)x_0$ which also lies in X_k.

In this section, we will show that, when $p \nmid k$, X_{k-1} is a transversal for the right cosets Dx satisfying $(\Delta_k\mathfrak{S}_p)^x \cap P \neq 1$. We begin with the observation that a transversal for these right cosets can be chosen to be a subset of X_{k-1}.

Proposition 6.1. *Let $k \in \mathbb{Z}^+$ with $p \nmid k$. Then $X_{k-1} \subseteq X_k$. Furthermore, if $x \in X_k$, then there exists $y \in X_{k-1}$ such that $Dx = Dy$.*

Proof. Let $\kappa = (\kappa_1, \kappa_2, \ldots, \kappa_l)$ be the p-adic p-composition of k. Since $p \nmid k$, we see that $\kappa_l = 0$, and $(\kappa_1, \ldots, \kappa_{l-1})$ is the p-adic p-composition of $(k-1)$. Thus, $X_k = X_{k-1} \times X_1[k]$ by Lemma 5.7(2). The first assertion now follows as 1 $(= z_{0,1})$ belongs to X_1.

For the second assertion, we have $x = a \cdot x'[k]$ where $a \in X_{k-1}$ and $x' = hz_{0,t}$ with $h \in H_1$ and $t \in \mathbb{Z}_p^*$. Let u be the inverse of t in $\mathbb{Z}_p^*$. Then $z_{0,u}$ is the inverse of $z_{0,t}$ by Lemma 5.4(2). Define $y := \Delta_{k-1}(z_{0,u}h^{-1})a$. Then $y \in Dx$ since $\Delta_k(z_{0,u}h^{-1}) \in D$ and

$$\Delta_k(z_{0,u}h^{-1})x = \Delta_{k-1}(z_{0,u}h^{-1})a \cdot (z_{0,u}h^{-1}x')[k] = y.$$

Furthermore, $y \in X_{k-1}$; to see this, note that $\Delta_{k-1}z_{0,u}$ normalises H_{k-1} and use Lemma 5.4(2). □

Before we continue, we make the following observation:

Lemma 6.2. *Let $m \in \mathbb{Z}_{\geq 0}$, and let $k \in \mathbb{Z}^+$ with p-adic p-composition $(\kappa_1, \ldots, \kappa_l)$. Then*

(1) $\mathfrak{S}_{p^m}^{[p]} \cap \prod_{i=1}^p \mathfrak{S}_{p^m}[i] = \prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i]$;
(2) $\mathfrak{S}_k^{[p]} \cap \prod_\kappa \mathfrak{S}_{p^{\kappa_i+1}} = \prod_\kappa \mathfrak{S}_{p^{\kappa_i}}^{[p]}$.

Proof. Note first that $\mathfrak{S}_{p^m}^{[p]}$ consists *precisely* of the permutations of $\mathfrak{S}_{p^{m+1}}$ which, in the natural action, induce row permutations on the tableau T. Suppose that $\sigma^{[p]} \in \prod_{i=1}^p \mathfrak{S}_{p^m}[i]$ for some $\sigma \in \mathfrak{S}_{p^m}$. Then $\sigma^{[p]}$ leaves each successive block in $[1, p^{m+1}]$ of size p^m invariant. Thus, on the tableau T, $\sigma^{[p]}$ leaves each of the p sub-tableaux consisting of p^{m-1} successive rows of T invariant setwise, so that $\sigma^{[p]} \in \prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i]$. This shows $\mathfrak{S}_{p^m}^{[p]} \cap \prod_{i=1}^p \mathfrak{S}_{p^m}[i] \subseteq \prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i]$. The converse clearly holds, since $\mathfrak{S}_{p^{m-1}}^{[p]} \subseteq \mathfrak{S}_{p^m}$ and

$$\prod_{i=1}^p \mathfrak{S}_{p^{m-1}}^{[p]}[i] = (\prod_{i=1}^p \mathfrak{S}_{p^{m-1}}[i])^{[p]} \subseteq \mathfrak{S}_{p^m}^{[p]}.$$

This proves part (1). Part (2) is similar. □

Proposition 6.3. *Let $k \in \mathbb{Z}^+$ such that $p \nmid k$, with p-adic p-composition $\kappa = (\kappa_1, \kappa_2, \ldots, \kappa_l)$. For each $i \in [1, l)$, let $x_i, y_i \in X_{p^{\kappa_i}}$. Let $x_l = y_l = 1$, and let $x = \prod_\kappa x_i$ and $y = \prod_\kappa y_i$. The following statements are equivalent:*

(1) $\mathfrak{S}_{p^{\kappa_i}}^{[p]} x_i = \mathfrak{S}_{p^{\kappa_i}}^{[p]} y_i$ *for all* $i \in [1, l)$;
(2) $\mathfrak{S}_k^{[p]} x = \mathfrak{S}_k^{[p]} y$;
(3) $Dx = Dy$.

Proof. (1) ⇒ (2) and (2) ⇒ (3) follow from the fact that

$$\prod_\kappa \mathfrak{S}_{p^{\kappa_i}}^{[p]} \subseteq \mathfrak{S}_k^{[p]} \subseteq D.$$

(3) $\Rightarrow$ (1): Suppose that $Dx = Dy$. Then there exist $\sigma \in \mathfrak{S}_k$ and $\tau \in \mathfrak{S}_p$ such that

$$(*) \qquad \sigma^{[p]}(\Delta_k \tau) \prod_{\kappa} x_i = \prod_{\kappa} y_i.$$

This gives

$$\sigma^{[p]} = \prod_{\kappa} (y_i x_i^{-1} (\Delta_{p^{\kappa_i}} \tau)^{-1}) \in \prod_{\kappa} \mathfrak{S}_{p^{\kappa_i+1}},$$

so that $\sigma^{[p]} \in \prod_\kappa \mathfrak{S}_{p^{\kappa_i}}^{[p]}$ by Lemma 6.2(2). Thus, for each $i \in [1, l]$ there exists $\sigma_i \in \mathfrak{S}_{p^{\kappa_i}}$ such that $\sigma^{[p]} = \prod_\kappa \sigma_i^{[p]}$. Putting this into $(*)$, we get, for all $i \in [1, l]$,

$$\sigma_i^{[p]} (\Delta_{p^{\kappa_i}} \tau) x_i = y_i.$$

When $i = l$, we have $\sigma_l = 1$ since $\kappa_l = 0$, and hence $\tau = 1$, since $x_l = y_l = 1$. Thus, we have, for $i \in [1, l)$,

$$y_i = \sigma_i^{[p]} x_i \in \mathfrak{S}_{p^{\kappa_i}}^{[p]} x_i.$$

□

In view of Proposition 6.3, our problem reduces to determining the necessary and sufficient conditions for $\mathfrak{S}_{p^m}^{[p]} x = \mathfrak{S}_{p^m}^{[p]} y$ where $x, y \in X_{p^m}$.

Recall that X_{p^m} is a disjoint union of Y_m and $\prod_{i=1}^p X_{p^{m-1}}[i]$ (Lemma 5.7(1)). We consider these two sets separately.

Proposition 6.4. *Let $m \in \mathbb{Z}^+$ and for each $i \in [1, p]$, let $x_i, y_i \in X_{p^{m-1}}$. The following statements are equivalent:*

(1) $\mathfrak{S}_{p^m}^{[p]} (\prod_{i=1}^p x_i[i]) = \mathfrak{S}_{p^m}^{[p]} (\prod_{i=1}^p y_i[i])$.
(2) $\mathfrak{S}_{p^{m-1}}^{[p]} x_i = \mathfrak{S}_{p^{m-1}}^{[p]} y_i$ *for all* $i \in [1, p]$.

The proof of this is straightforward, using Lemma 6.2(1). It remains to consider the right cosets $\mathfrak{S}_{p^m}^{[p]} x$ where $x \in Y_m$.

Proposition 6.5. *Let $m \in \mathbb{Z}_{\geq 0}$. Suppose that there exist $x \in X_{p^m}$ and $y \in Y_m$ such that $\mathfrak{S}_{p^m}^{[p]} x = \mathfrak{S}_{p^m}^{[p]} y$. Then $x = y$.*

Proof. We have $y = \tau^{[p]} x$ for some $\tau \in \mathfrak{S}_{p^m}$. Since $y \in Y_m$, we have $(\Delta_{p^m} \pi)^y \in R_m \setminus B_m$, and since $\tau^{[p]}$ centralises $\Delta_{p^m} \pi$ we have

$$(\Delta_{p^m} \pi)^x = (\Delta_{p^m} \pi)^y \in R_m \setminus B_m.$$

We claim that $x \in Y_m$. If not, then $x \in \prod_{i=1} X_{p^{m-1}}[i] \subseteq \prod_{i=1}^p \mathfrak{S}_{p^m}[i]$, say $x = \prod_{i=1}^p x_i[i]$, and then $(\Delta_{p^m} \pi)^x = \prod_{i=1}^p (\Delta_{p^{m-1}} \pi)^{x_i}[i] \in \prod_{i=1}^p \mathfrak{S}_{p^m}[i]$, a contradiction since $(R_m \setminus B_m) \cap \prod_{i=1}^p \mathfrak{S}_{p^m}[i] = \emptyset$. Thus $x \in Y_m$ and hence $x = y$ by the uniqueness result of Proposition 5.5. □

Theorem 6.6. *Let $k \in \mathbb{Z}^+$ with $p \nmid k$. Then X_{k-1} is a transversal of the right cosets Dx satisfying $(\Delta_k \mathfrak{S}_p)^x \cap P \neq 1$.*

Proof. This follows from Propositions 6.1, 6.3, 6.4 and 6.5. □

Corollary 6.7.

(1) *Let $m \in \mathbb{Z}_{\geq 0}$, and let $a_m = |X_{p^m}|$. Then a_m satisfies the following recurrence relation (where $a_{-1} = 0$):*
$$a_m = a_{m-1}^p + p^{2p^m - 1}(p-1).$$

(2) *Let $k \in \mathbb{Z}^+$ such that $p \nmid k$, with p-adic p-composition $(\kappa_1, \dots, \kappa_l)$. Then $|X_{k-1}| = \prod_{i=1}^{l-1} a_{\kappa_i}$. In particular,*
$$\dim((\operatorname{Res}_P \operatorname{Lie}(kp))_{pf}) = (p-1)(k-1)! \prod_{i=1}^{l-1} a_{\kappa_i}.$$

Proof. From the uniqueness of Proposition 5.5, we have
$$|Y_m| = |H_{p^m}||\mathbb{Z}_p^*||R_{m-1}|^{p-1} = p^{2p^m-1}(p-1)$$
(note that $|R_{m-1}| = p^{\frac{p^m-1}{p-1}}$). The Corollary follows now from Lemma 5.7, Theorem 6.6 and Corollary 3.6. □

Theorem 6.8. *Let $k \in \mathbb{Z}^+$ with $p \nmid k$. Then $e^{C_1 k} \leq |X_{k-1}| \leq e^{C_2 k}$ is for some constants $C_1 < C_2$.*

In particular, the dimension of $(\operatorname{Res}_P \operatorname{Lie}(kp))_{pf}$ grows exponentially with k, but $\dim((\operatorname{Res}_P \operatorname{Lie}(kp))_{pf}) / \dim(\operatorname{Lie}(kp)) \to 0$ as $k \to \infty$.

Proof. Let $\kappa = (\kappa_1, \dots, \kappa_l)$ be the p-adic p-composition of k. Then κ is a p-regular partition (i.e. it is weakly decreasing and does not have p or more equal parts), and $|X_{k-1}| = \prod_{i=1}^{l-1} a_{\kappa_i}$ by Corollary 6.7(2). It is not difficult to show by induction that $a_{\kappa_1} \leq \prod_{i=1}^{l-1} a_{\kappa_i} \leq a_{\kappa_1+1}$, and that a_m is of order p^{2p^m}. Thus $e^{C_1 k} \leq |X_{k-1}| \leq e^{C_2 k}$ for some constants $C_1 < C_2$.

Since $\dim((\operatorname{Res}_P \operatorname{Lie}(kp))_{pf}) = (p-1)(k-1)!|X_{k-1}|$, and $m!$ is of order $e^{m \log m}$, we see that $\dim(\operatorname{Res}_P \operatorname{Lie}(kp))_{pf}$ grows exponentially with k, and $\dim(\operatorname{Res}_P \operatorname{Lie}(kp))_{pf} / \dim(\operatorname{Lie}(kp)) \to 0$ as $k \to \infty$. □

Theorem 6.8 thus lends some support to the belief that $\operatorname{Lie}^{\max}(kp)$ is relatively large compared with $\operatorname{Lie}(kp)$, as mentioned in our introduction, even though $\operatorname{Lie}(kp)_{pf}$ grows exponentially with k.

Remark. Selick and Wu [SW2] computed explicitly $\operatorname{Lie}^{\max}(6)$ and $\operatorname{Lie}^{\max}(8)$ in characteristic two. In particular, they showed that $\operatorname{Lie}^{\max}(6)$ has dimension 96, which is also the upper bound computed by our recurrence formula.

References

[AK] G. Arone, M. Kankaanrinta, 'The homology of certain subgroups of the symmetric group with coefficients in Lie(n)', *J. Pure Appl. Algebra* **127** (1–14), 1998.

[AM] G. Arone, M. Mahowald, 'The Goodwillie tower of the identity functor and the unstable periodic homotopy of spheres', *Invent. Math.* **135** (743–788), 1999.

[B] D.J. Benson, 'Representations and cohomology I: Basic representation theory of finite groups and associative algebras', *Cambridge Studies in Advanced Mathematics* **30**, CUP, 1991.

[C] F. Cohen, 'The homology of $\mathcal{C}_{n+1}$ spaces, $n \geq 0$', in: Homology of Iterated Loop Spaces, in: Lecture Notes in Mathematics **533**, Springer, 1976.

[ES] K. Erdmann, M. Schocker, 'Modular Lie powers and the Solomon descent algebra', *Math. Z.* **253** (295–313), 2006.

[SW1] P. Selick, J. Wu, 'Natural coalgebra decomposition of tensor algebras and loop suspensions', *Mem. Amer. Math. Soc.* **148**, 2000.

[SW2] P. Selick, J. Wu, 'Some calculations for $\mathrm{Lie}(n)^{\max}$ for low n', *J. Pure Appl. Algebra* **212** (2570–2580), 2008.

[We] F. Weber, 'Über invarianten in Lieschen Ringen', *Math. Ann.* **120** (563–580), 1949.

[Wi] E. Witt, 'Über freie Liesche Ringe und ihre Unterringe', *Math. Z.* **56** (195–216), 1956.

(K. Erdmann) Mathematical Institute, 24–29 St Giles', Oxford, OX1 3LB, United Kingdom.

E-mail address: `erdmann@maths.ox.ac.uk`

(K. M. Tan) Department of Mathematics, National University of Singapore, 2, Science Drive 2, Singapore 117543.

E-mail address: `tankm@nus.edu.sg`